ID: 491287
Sample Name:
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Cookbook: default.jbs
Time: 12:40:43
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

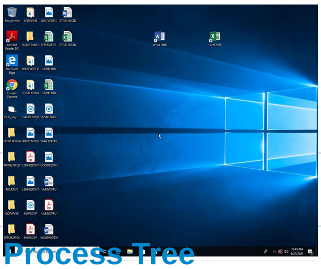
Windows Analysis Report DHL_Shipment_Notification_…

Overview

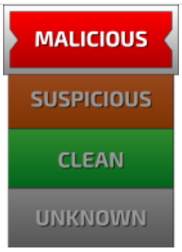
General Information

Sample Name:	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Analysis ID:	491287
MD5:	8e2b177d2ab29c..
SHA1:	f347fa229d51836..
SHA256:	b9fdde7d748e27a.
Tags:	DHL exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



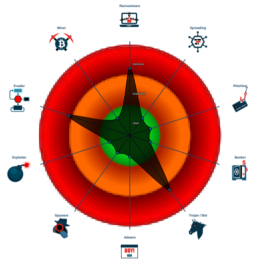
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Found potential dummy code loops (…
- Uses 32bit PE files
- Contains functionality to call native f…
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Program does not show much activi…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe (PID: 6996 cmdline: 'C:\Users\user\Desktop\DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe' MD5: 8E2B177D2AB29C95F067559A029CF5E8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.872323022.0000000002BE0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

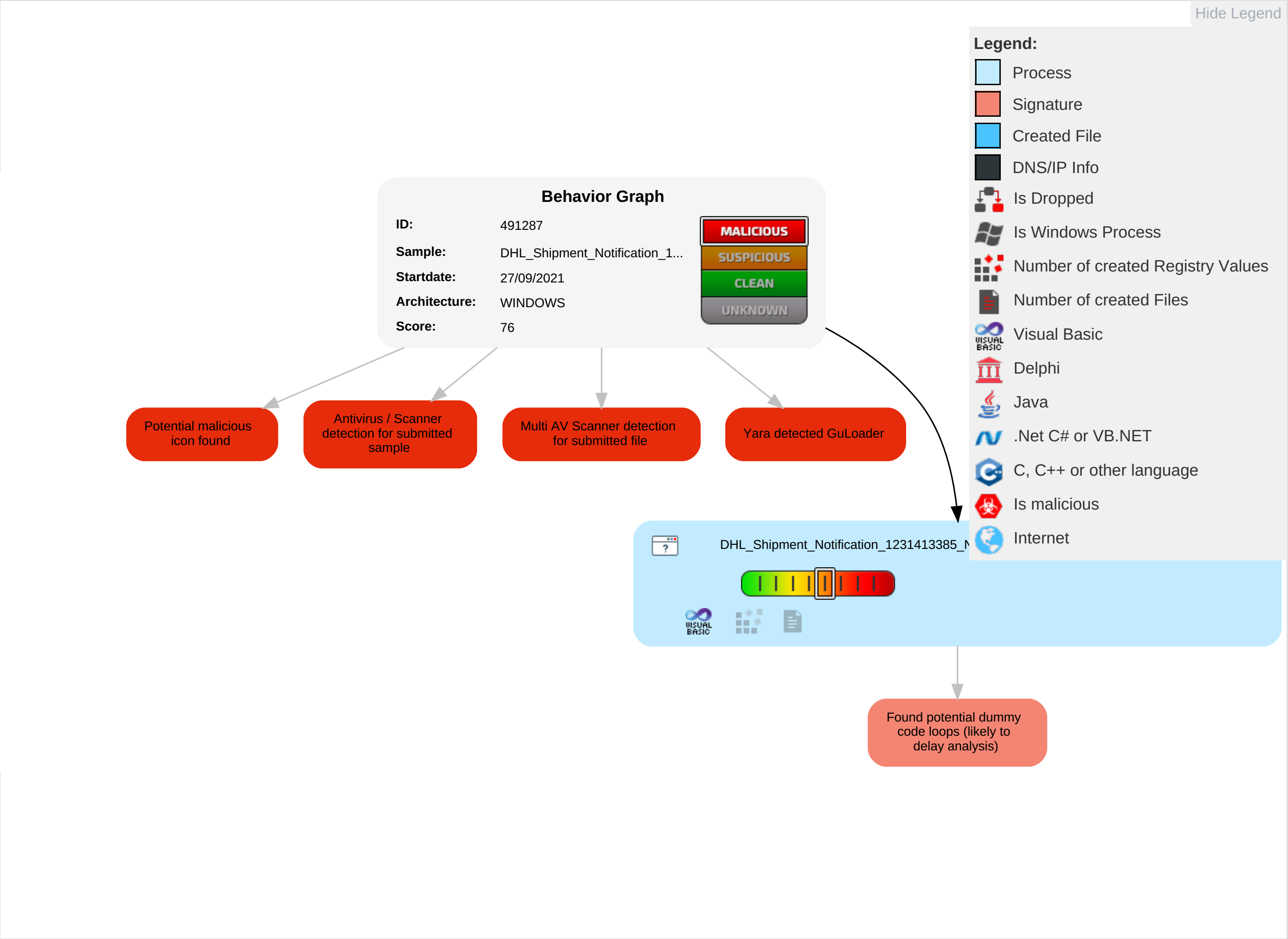
Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



Hide Legend

Legend:

- ⬜ Process
- 🟥 Signature
- 🟦 Created File
- ⬛ DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Behavior Graph

ID:	491287
Sample:	DHL_Shipment_Notification_1...
Startdate:	27/09/2021
Architecture:	WINDOWS
Score:	76

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Potential malicious icon found

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Yara detected GuLoader

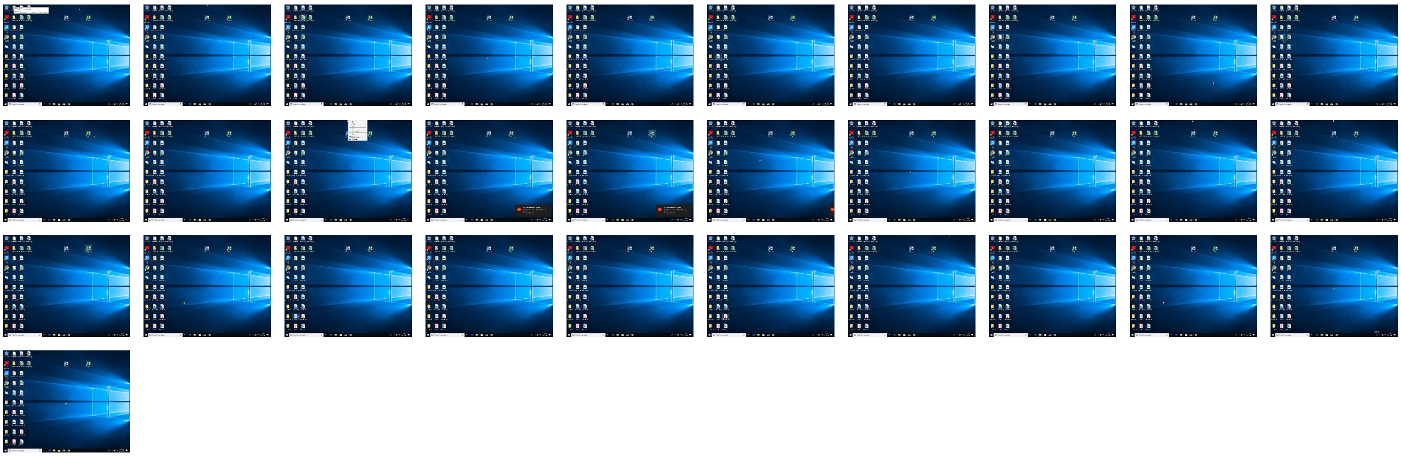
DHL_Shipment_Notification_1231413385_N

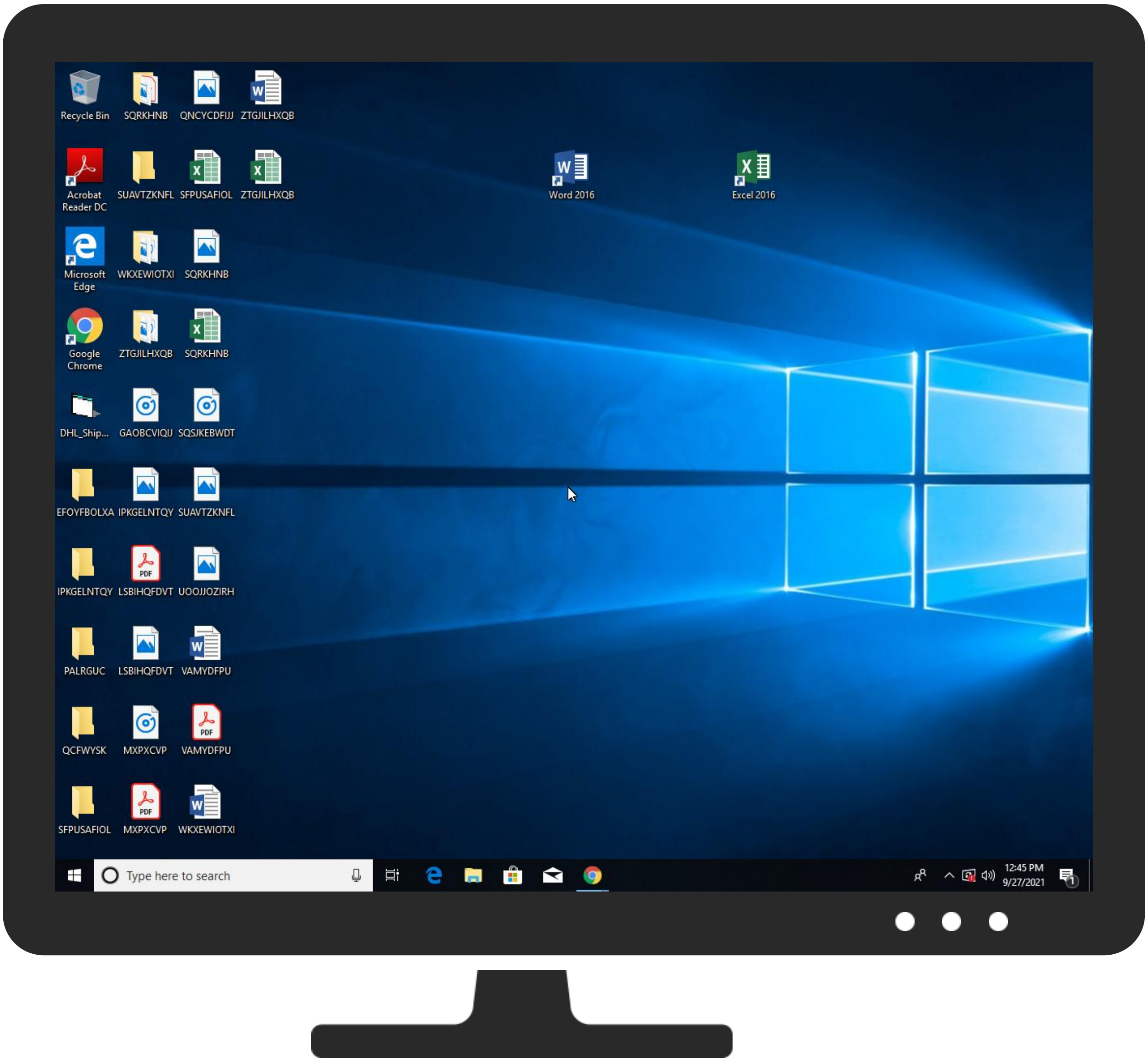
Found potential dummy code loops (likely to delay analysis)

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	32%	Virustotal		Browse
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	18%	ReversingLabs	Win32.Trojan.Mucc	
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	100%	Avira	HEUR/AGEN.1141869	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141869		Download File
0.0.DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141869		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491287
Start date:	27.09.2021
Start time:	12:40:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 1.2%) • Quality average: 50.8% • Quality standard deviation: 27.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.804544485598051
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
File size:	98304
MD5:	8e2b177d2ab29c95f067559a029cf5e8
SHA1:	f347fa229d51836344ab5bf89fa531e19aa5e324
SHA256:	b9fdde7d748e27a130c509a589a2c8b92aad279604d3e4ee7ac28187fc5660be
SHA512:	29493bc83ab2348c5f3f707079e968302e03256acd3801c9c5e47c13a87cb9ec70145208bb25a4127e30cbe2cd7edca1a6cd82a23ca7a5e5a8a0bb0a19e1aa00
SSDEEP:	768:37nneTCCOKskAtEcDpHR0QWNTsO85zCoLi/0Fqt1fgg9ZPxt/ZbwKbdU5p0:TnWAT4sO87LFIl3Ph2c
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........,..SM..SM..SM...Q..RM...o..uM..ek..RM..RichSM..................PE..L......I.................P...@...............`....@........

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4012f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x49E892D2 [Fri Apr 17 14:31:46 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	508f324e8f3f3b33e0170cdca30d1edb

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x141f0	0x15000	False	0.50043015253	data	6.21499607809	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0x205c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x8e4	0x1000	False	0.169921875	data	1.92865182643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe PID: 6996 Parent PID: 4688

General

Start time:	12:41:43
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	8E2B177D2AB29C95F067559A029CF5E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.872323022.0000000002BE0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis